DELL Technologies

Passerelle de connexion sécurisée

Notre technologie intègre la protection des données et la prévention des menaces dans une expérience de support automatisée et sécurisée

Jusqu'à

60 %

des leaders IT interrogés par Forrester utilisent la technologie de connectivité pour réduire les risques[1]

Elle est également implémentée pour la connexion directe de certains matériels Dell EMC et un plug-in de services dans OpenManage Enterprise pour les serveurs PowerEdge. Dell Technologies Services s'engage à mettre en œuvre des fonctionnalités de sécurité basées sur les marchés, les réglementations et les informations client, qui aident nos produits à répondre aux objectifs de sécurité et aux exigences de conformité de nos clients.

Contenu

1. Introduction

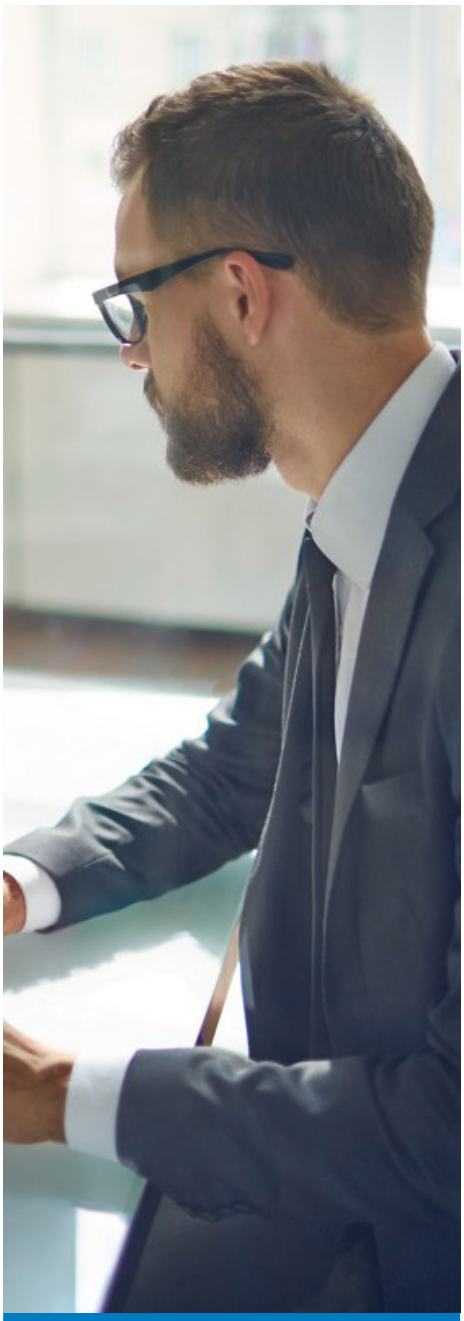
Dans le monde hyper-numérique actuel, les leaders de l'innovation qui réussissent se tournent vers les prestataires de services informatiques pour sous-traiter le support informatique. Selon une étude de Forrester Consulting réalisée à la demande de Dell Technologies Services[1], 59 % des leaders informatiques indiquent qu'un partenariat avec le bon prestataire de services informatiques leur permet de transférer le temps que le personnel informatique consacre aux opérations quotidiennes vers l'innovation et des initiatives stratégiques.

En tant que prestataire de services informatiques de premier plan, Dell Technologies Services s'engage à veiller à ce que ses services et technologies de support informatique n'engendrent pas de menaces potentielles sur la sécurité. Chaque jour, nous faisons tout notre possible afin de minimiser les risques pour nos clients liés aux produits Dell EMC déployés dans leur environnement. Ce document explore la manière dont la sécurité est intégrée à la conception, à l'implémentation et au fonctionnement de la passerelle de connexion sécurisée afin de garantir une expérience de support informatique automatisée et sécurisée pour l'infrastructure de datacenter complexe.

S'appuyant sur plus de 25 ans de technologie de support informatique innovante, l'architecture de sécurité de la passerelle de connexion sécurisée est conçue pour éviter les incursions des menaces et protéger l'intégrité des données. Notre technologie surveille en permanence les appareils des clients pour résoudre les problèmes et initier une résolution accélérée, mais en plus de cela :

- Nous utilisons uniquement des données de télémétrie et d'événements issues de systèmes actifs.
- Nous chiffrons les données d'état du système pour le transport via Internet sur HTTPS à l'aide du protocole TLS (Transport Layer Security).
- Nos ingénieurs du support technique agréés utilisent l'authentification multifacteur pour accéder aux systèmes connectés à distance et résoudre les problèmes.
- Nous traitons, stockons et utilisons les données de télémétrie et d'événements sur nos sites à l'aide de pratiques de sécurité de pointe.

De plus, nous respectons rigoureusement les mesures de sécurité intégrées à l'architecture et aux processus de la passerelle de connexion sécurisée avec plusieurs fournisseurs haut de gamme, tels que Secureworks, pour vous garantir une expérience sécurisée et confidentielle.



Les cyberattaques et la fraude ou le vol de données figurent parmi les dix principales préoccupations des PDG[2]

2. À propos de la Passerelle de connexion sécurisée

Dell Technologies propose une technologie de connectivité sécurisée qui élimine les conjectures en matière de prévention des problèmes. Vous avez ainsi plus de temps pour vous concentrer sur les projets les plus importants. Les éditions d'appliance virtuelle et d'application assurent une connexion bidirectionnelle sécurisée entre votre environnement et Dell Technologies Services, idéale pour surveiller les appareils Dell EMC dans votre datacenter, y compris le stockage de données, les serveurs, la gestion de réseau, les infrastructures convergées/hyperconvergées et la protection des données, le tout à un seul et même endroit.

Vous pouvez également déployer notre technologie de manière flexible en tant que version de connexion directe pour certains produits Dell EMC et avec un plug-in Services dans OpenManage Enterprise pour les serveurs PowerEdge. Dell.com/Support pour vérifier les options de connectivité prises en charge sur le matériel et les logiciels Dell EMC spécifiques.

Les données sont l'élément de base de la passerelle de connexion sécurisée. Nous tirons parti des données de l'état du système dans les environnements des clients. Nous les corrélons avec des années de données d'incident et d'ingénierie issues des équipes de support technique et de terrain, ainsi que des fabricants de composants.

Affichez les éléments pouvant faire l'objet d'un rapport pour la Passerelle de connexion sécurisée et le plug-in Services pour OpenManage Enterprise afin d'avoir plus de détails sur les informations collectées sur l'état du système.

En utilisant des modèles d'intelligence artificielle sophistiqués, notamment l'apprentissage automatique, notre technologie de connectivité peut trouver et appliquer des schémas pour détecter avec précision le problème à prendre en compte dès la première fois. Elle identifie les problèmes matériels et logiciels, crée un incident et nous contacte pour que nous puissions commencer à résoudre les problèmes avant qu'ils ne deviennent onéreux. Elle prédit les défaillances sur les disques durs et les fonds de panier lorsque le système est connecté via la passerelle de connexion sécurisée. En fonction du type de problème, l'alerte peut également déclencher une expédition automatique de pièces.

En outre, la technologie permet une communication bidirectionnelle sécurisée pour les agents du support technique autorisés à accéder à distance aux appareils gérés, afin de résoudre les problèmes et les incidents.

SÉCURITÉ POUR LA CONNECTIVITÉ

Les évaluations de sécurité tierces sont effectuées régulièrement par rapport à la passerelle de connexion sécurisée et à son infrastructure de prise en charge.

Les évaluations des applications incluent notamment le transport des données et la sécurité des API, l'analyse des codes source statiques et dynamiques, les failles de sécurité courantes et les expositions (CVE, Common Vulnerabilities and Exposures) et les vérifications croisées OWASP (Open Web Application Security Project), ainsi que les bibliothèques et produits tiers.

Les évaluations de l'infrastructure sont notamment les périphériques, serveurs et prestataires de services internes et externes du réseau.

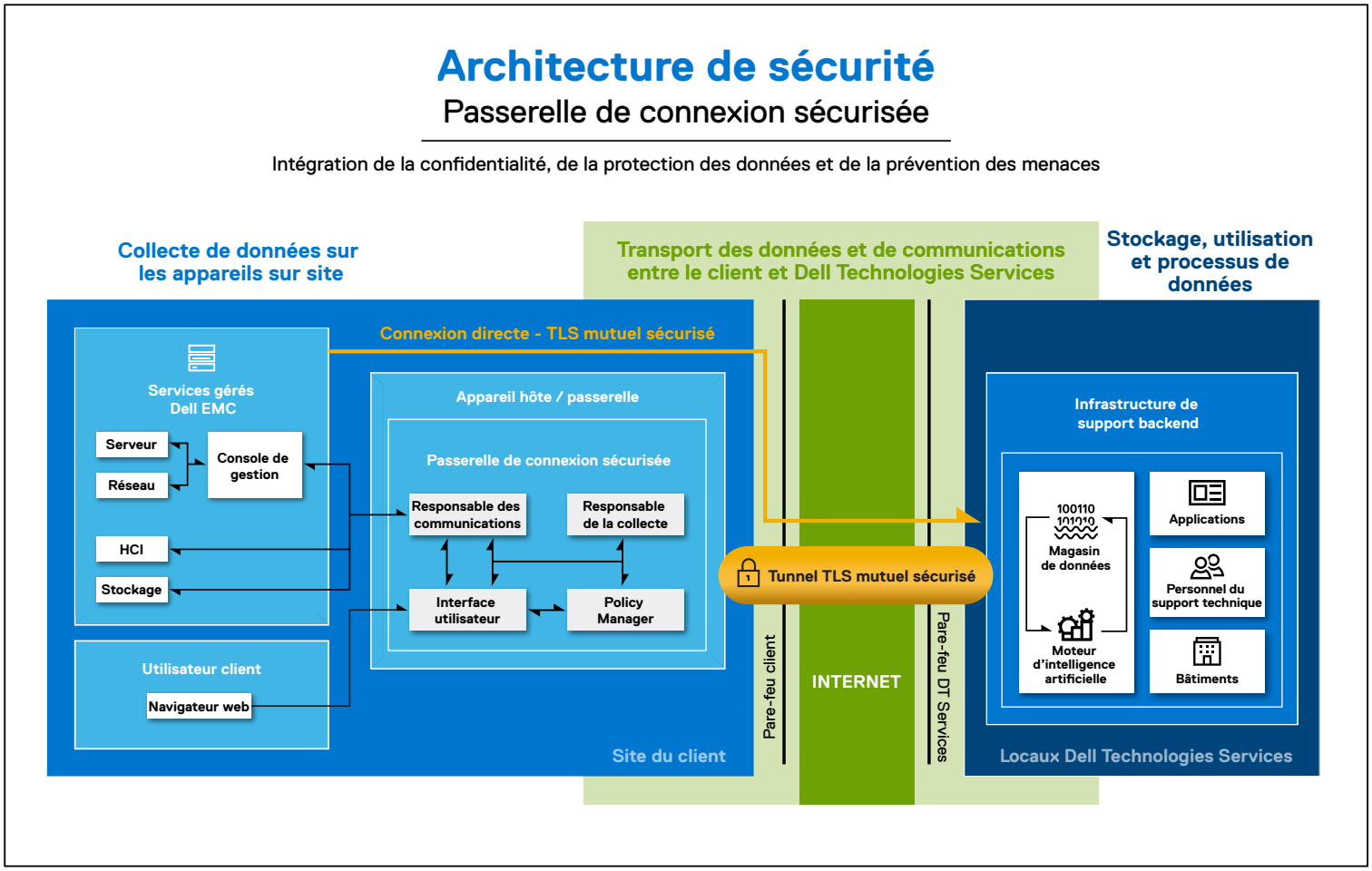
3. Présentation de l'architecture de sécurité

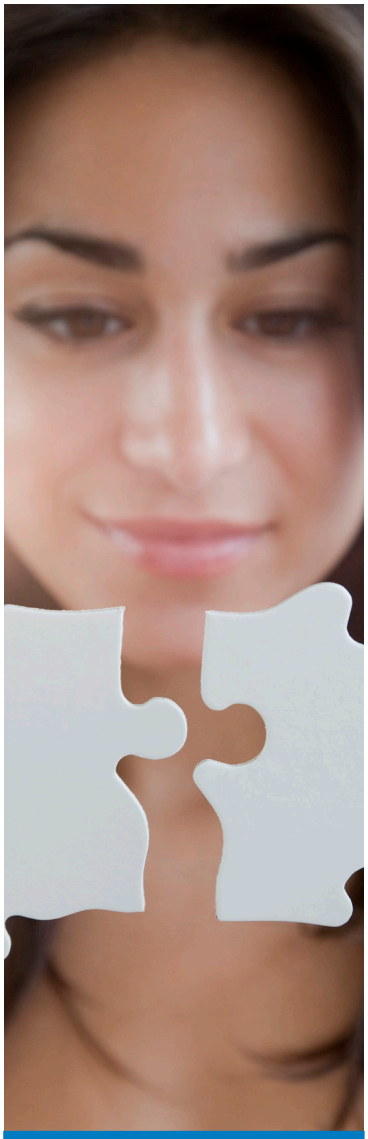
Dell Technologies Services s'engage à minimiser les risques de menaces de sécurité au sein de notre technologie de connectivité à la fois proactive et prédictive. Notre architecture de sécurité repose sur des normes rigoureuses du secteur et adhère à des pratiques de sécurité mesurables et reproductibles à chaque étape du développement et du déploiement des produits. Pour plus d'informations, consultez la section 4.

Le diagramme A ci-dessous présente l'architecture de sécurité de la passerelle de connexion sécurisée. Dans les sections suivantes, nous allons détailler comment notre technologie ne recueille que les données système des appareils gérés par Dell EMC nécessaires pour diagnostiquer et résoudre les problèmes, puis gère ces données avec une sécurité et une confidentialité maximales lors des étapes suivantes :

- Collecte de données sur les appareils sur site
- Transport et communication des données
- Stockage, utilisation et processus de données au sein de Dell Technologies Services

Diagramme A :





Les clients bénéficient d'une couche de sécurité supplémentaire pour la collecte de données sur site via les fonctionnalités d'audit de Policy Manager dans la passerelle de connexion sécurisée

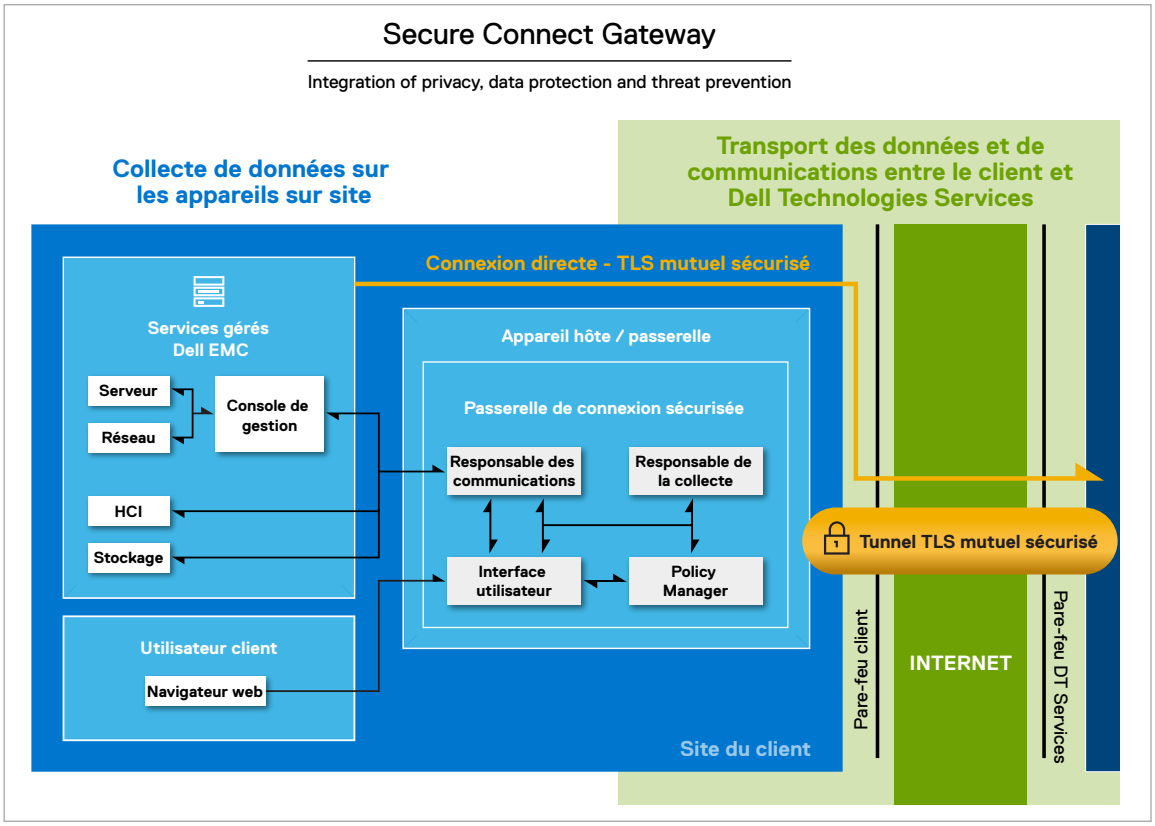
4. Approche détaillée de la sécurité pour la Passerelle de connexion sécurisée

4-1. Collecte sécurisée des données sur site

Réduction des points d'accès au pare-feu

La passerelle de connexion sécurisée regroupe les communications entre les appareils Dell EMC et agit comme un point d'entrée et de sortie unique dans le pare-feu d'un client pour toutes les activités de services à distance basées sur IP. Reportez-vous au diagramme B. En minimisant les points d'accès du pare-feu pour la technologie de support informatique à distance, Dell Technologies réduit les risques de sécurité via le pare-feu de l'entreprise.

Diagramme B : (extrait du diagramme A – architecture de sécurité) :



En tant que passerelle sur site, la passerelle de connexion sécurisée est déployée virtuellement sur un hyperviseur fourni par le client. Chaque serveur de passerelle agit comme un proxy, transportant des informations depuis et vers des appareils gérés. La passerelle de connexion sécurisée peut également mettre en file d'attente les événements de connexion à domicile en cas de défaillance d'un réseau local temporaire. Ces serveurs de passerelle disposent de leur propre interface utilisateur Web basée sur le système d'exploitation sous-jacent.

Pour certains clients, la version de connexion directe est adaptée au déploiement hétérogène de plusieurs produits matériels Dell EMC. Cette solution agit comme un point de communication sécurisé unique via le pare-feu du client. Il est intégré à l'environnement d'exploitation du produit et ne nécessite donc pas de serveur distinct pour fournir un support à distance entrant et une fonctionnalité d'appel à domicile.

Réduction des points d'accès au pare-feu (suite)

Pour les clients d'un datacenter PowerEdge utilisant la console de gestion des systèmes OpenManage Enterprise, le plug-in Services intégré représente une option d'implémentation alternative. Ce plug-in de connectivité au sein de l'appliance virtuelle OpenManage Enterprise s'exécute sur un hyperviseur fourni par le client. Il agit comme une couche d'automatisation des services à partir d'appareils de serveur et de châssis gérés, et fournit une connexion directe unique et sécurisée au back-end Dell Technologies Services.

Véritable courtier en communications sécurisé

La passerelle de connexion sécurisée agit en tant que courtier en communications entre les appareils gérés, Policy Manager et l'infrastructure de support back-end de Dell Technologies Services. Les serveurs de passerelle sur lesquels il est déployé sont des gestionnaires HTTPS. Les serveurs de passerelle utilisent différentes méthodes de communication, notamment la détection des appareils, la gestion des événements, la collecte de données de télémétrie et la gestion des données de télémétrie. Les types de messages sont les suivants :

- Interrogation des pulsations de l'état de l'appareil
- Transfert de fichiers de données (connexion à domicile)
- Transfert des données d'utilisation des licences
- Demandes d'authentification utilisateur
- Synchronisation de la gestion des appareils

Tous les messages sont sécurisés à l'aide de plusieurs protocoles. Dans une section à venir, nous allons examiner de plus près la sécurité supplémentaire intégrée à la communication et au transport de données de la passerelle de connexion sécurisée, notamment l'utilisation du protocole HTTPS avec la tunnelisation du protocole TLS de bout en bout et le chiffrement standard du secteur.

Contrôle client des exigences d'autorisation et des autorisations d'accès

Si les appareils sont surveillés par la passerelle de connexion sécurisée dans le datacenter d'un client, celui-ci peut choisir d'utiliser Policy Manager afin de contrôler les exigences d'autorisation pour les connexions d'accès distant, les exécutions de scripts de diagnostic et d'autres activités connexes. Les clients peuvent définir des autorisations d'accès pour le personnel et les ingénieurs du support technique, qui se connectent à distance pour diagnostiquer et résoudre les problèmes.

La sécurité pour la gestion des autorisations est assurée par les fonctions Policy Manager suivantes :

- La passerelle de connexion sécurisée interroge régulièrement Policy Manager pour connaître les modifications apportées aux autorisations et met en cache les autorisations en local. Dans le cas de Policy Manager :
  - Le cache de jeu de règles est automatiquement mis à jour avec les mises à jour de configuration après le dernier cycle d'interrogation.
  - Il est configuré pour recevoir des messages en tant qu'écouteur HTTPS sur un port spécifique et approuvé.
- Lorsque la passerelle de connexion sécurisée reçoit une demande d'accès distant ou toute autre action, elle applique la politique reçue à partir du cache de Policy Manager.
  - Les autorisations peuvent être attribuées de manière hiérarchique à des politiques basées sur des types d'appareils ou des modèles spécifiques dans un type d'appareil.
  - Les clients peuvent accepter ou refuser l'action demandée via l'interface utilisateur Web de Policy Manager. Ils peuvent également créer des filtres pour définir d'autres restrictions sur les autorisations et les actions.

Journalisation et pistes d'audit

Les clients bénéficient d'une couche de sécurité supplémentaire pour la collecte de données sur site via les fonctionnalités d'audit de Policy Manager dans la passerelle de connexion sécurisée. Policy Manager enregistre tous les événements et connexions des services distants, les exécutions de scripts de diagnostic et les opérations de transfert de fichiers de support. Il les stocke ensuite dans sa base de données sous forme de fichiers journaux d'audit à texte plat. Il suit l'accès à lui-même (Policy Manager), les modifications de politique et toutes les activités d'autorisation ou de refus d'accès.

Les clients disposent de toutes ces informations à portée de main :

- Les audits sont affichés via l'interface utilisateur Web de Policy Manager et ne peuvent pas être modifiés.
- Les journaux d'audit peuvent également être configurés pour être transmis à un serveur syslog dans leur environnement.

Passerelle de connexion sécurisée

Suites de chiffrement TLS 1.2 prises en charge :

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Option de sécurité de contrôle des appareils

Étant donné que les clients n'activent pas toujours Policy Manager pour la gestion des autorisations et des permissions, la passerelle de connexion sécurisée fournit des fonctions de sécurité connexes via l'option de contrôle des appareils.

Les clients peuvent :

- créer des groupes personnalisés en fonction du type d'appareil, du groupe d'administrateurs, de l'organisation ou de l'unité commerciale, de l'emplacement physique de l'appareil ou de tout autre critère choisi ;
- définir des autorisations et des droits d'accès spécifiques selon ces groupes d'appareils.

Toutes les opérations de gestion des appareils, y compris l'activité à distance par les ingénieurs du support technique, sont enregistrées. Elles doivent également être approuvées dans le backend par un agent du support technique.

De cette façon, les clients maintiennent un contrôle et une transparence complets sur les appareils gérés via la passerelle de connexion sécurisée.

Authentification à deux facteurs et gestion des certificats numériques

L'authentification est un composant important de la collecte sécurisée des données sur site. La passerelle de connexion sécurisée utilise un certificat numérique comme preuve d'identité de son déploiement sur le serveur de passerelle du client. Le certificat lie l'identité du serveur de passerelle à une paire de clés qui est utilisée pour chiffrer et authentifier la communication avec le back-end. L'autorité de certification de Dell Technologies Services est le référentiel central de l'infrastructure de clés de la passerelle de connexion sécurisée.

La gestion des certificats numériques permet d'automatiser l'inscription du certificat numérique par le biais de notre autorité de certification privée. Cela :

- permet la génération par programme et l'authentification de chaque demande de certificat ;
- garantit que le certificat est uniquement délivré et installé sur le serveur de passerelle. Le certificat ne peut pas être copié et utilisé sur une autre machine.

La passerelle de connexion sécurisée se connecte et s'authentifie à l'aide du certificat numérique déployé sur notre infrastructure de support back-end. Les agents du support technique se connectent à la passerelle de connexion sécurisée dans l'environnement du client à l'aide de l'authentification à deux facteurs.

4-2. Transport et communication sécurisés des données

Tunnel de communication sécurisé

Toutes les communications entre le client et l'infrastructure back-end de support Dell Technologies Services sont lancées en sortie par la passerelle de connexion sécurisée à partir du site du client. Il crée un tunnel de communication sécurisé de bout en bout à l'aide du chiffrement du protocole TLS 256 bits standard sur Internet, et de l'authentification par certificat numérique signée par Dell Technologies Services. Ce dernier point est détaillé dans la section précédente sur la collecte sécurisée des données sur site.

Ainsi, les connexions de la passerelle de connexion sécurisée possèdent les propriétés suivantes :

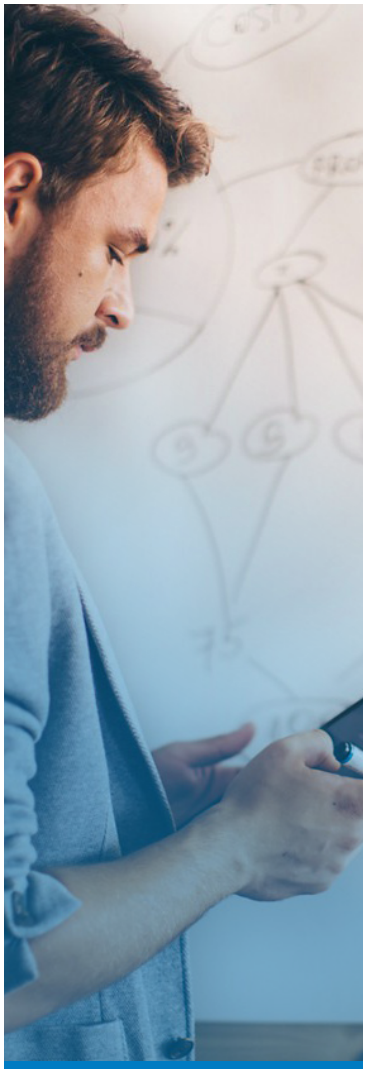
- **Transfert fiable des données :** chaque message transmis comprend une vérification de l'intégrité du message à l'aide d'un code d'authentification des messages, afin d'éviter toute perte ou altération non détectée des données lors de la transmission.
- **Session privée et sécurisée via TLS :** le chiffrement symétrique à l'aide d'algorithmes standard génère des clés uniques pour chaque connexion. Les communications ne peuvent pas être modifiées au cours de la négociation sans être détectées.
- **Parties authentifiées :** étant donné que cette connexion est sécurisée, elle identifie les parties communicantes et les authentifie à l'aide d'une cryptographie à clé publique. Cette approche empêche l'usurpation d'identité et les attaques man-in-the-middle (MITM).

Communications à l'aide du tunnel TLS sécurisé

Le serveur de passerelle utilise le tunnel TLS pour garantir un environnement sécurisé pour les fonctions suivantes : interrogation des pulsations, notification à distance et accès distant. Dans cette section et selon le diagramme C, nous étudions de plus près ces processus et protocoles de communication de base pour l'expérience automatisée, proactive et prédictive de notre technologie.

Interrogation des pulsations

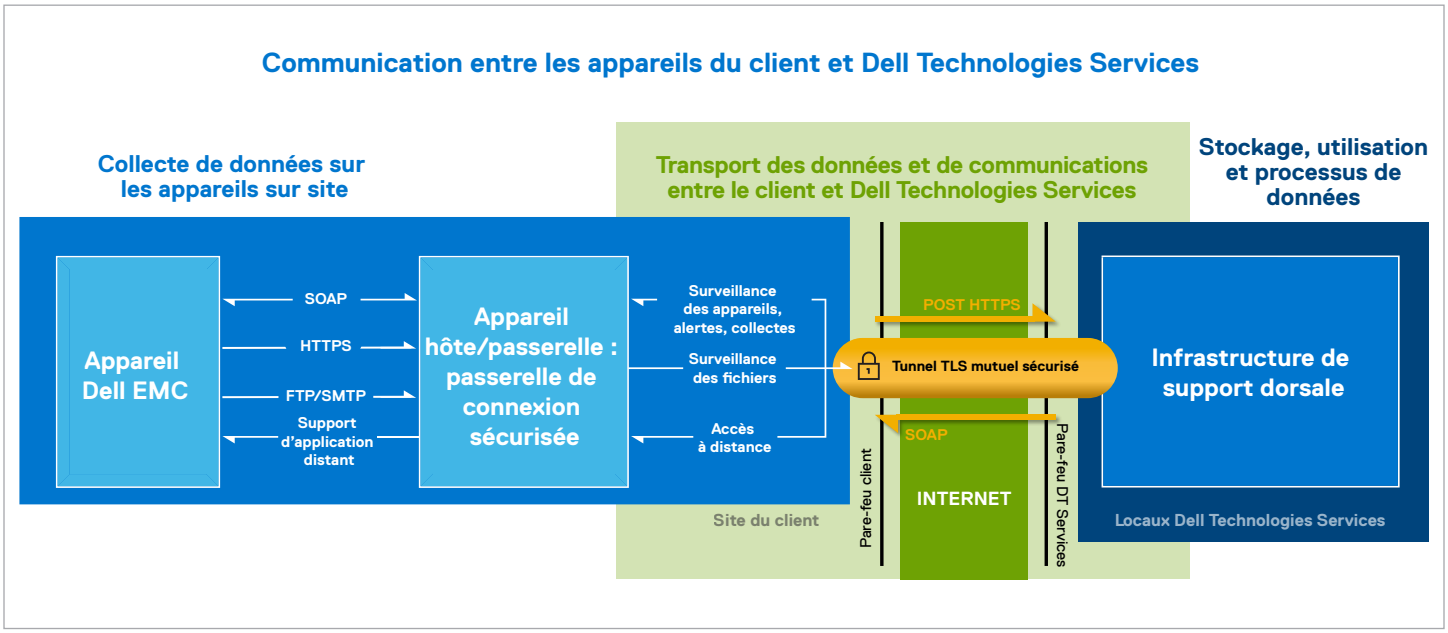
Les systèmes clients doivent être connectés pour bénéficier de l'expérience de la passerelle de connexion sécurisée. L'interrogation des pulsations vérifie l'état de connectivité des appareils et communique régulièrement les données de télémétrie collectées au back-end. Les données identifient également le serveur de passerelle sur lequel la passerelle de connexion sécurisée est déployée.



L'authentification de pointe sécurise les connexions contre l'usurpation d'identité et les attaques de type « man-in-the-middle »

Communications à l'aide du tunnel TLS sécurisé - Suite

Diagramme C : architecture de sécurité



Notification à distance ou fonction de connexion à domicile

La passerelle de connexion sécurisée sert d'intermédiaire sécurisé pour les appareils qui envoient des fichiers d'événements au back-end. Cela comprend les erreurs, les alertes, les conditions d'avertissement, les rapports d'intégrité, les données de configuration et les statuts d'exécution de script.

- Lorsqu'une alerte est générée, un fichier d'événement est généré et envoyé à la passerelle.
- Le fichier est reçu par la passerelle de connexion sécurisée via les services d'écouteur HTTPS.
- Les fichiers sont chiffrés et transférés pour les produits existants qui utilisent des écouteurs FTP et/ou SMTP pour la passerelle de connexion sécurisée.
- La passerelle compresse le fichier et l'envoie au back-end via le tunnel TLS. Il supprime ensuite le fichier du répertoire de l'écouteur.
- Le fichier est ensuite décompressé dans le backend pour analyse.
- La passerelle de connexion sécurisée peut également envoyer les fichiers au back-end via le tunnel de communication chiffré. De plus, la passerelle peut être configurée pour utiliser les canaux de basculement, à savoir FTPS ou le serveur de messagerie du client.

Les données de surveillance du système sont collectées à partir de divers composants d'un système actif afin de permettre à Dell Technologies Services de fournir une expérience de support adaptative, intelligente et accélérée. L'ID du système, qui est nécessaire pour identifier le système spécifique en cours d'utilisation, est la seule information sur l'entreprise collectée sur les appareils. Lorsque nous déterminons qu'une pièce doit être expédiée proactivement, nous utilisons les coordonnées existantes qui ont été stockées de manière sécurisée sur les serveurs Dell Technologies.

Vous trouverez la liste complète des données de surveillance du système collectées à partir d'un système actif, y compris les données collectées en dehors du cycle de routine de 24 heures, dans les documents Éléments pouvant faire l'objet d'un rapport pour Secure Connect Gateway et le plug-in Services pour OpenManage Enterprise.

Accès à distance

Nos équipes de support technique accèdent également à distance aux appareils sur un site client afin de résoudre les problèmes ou d'effectuer des actions spécifiques à l'appareil. La messagerie asynchrone garantit que la session d'accès distant est initialisée par la passerelle de connexion sécurisée à partir du site du client. Ensuite, une session d'accès à distance sécurisée est définie comme suit :

- Après l'authentification de la session au niveau du backend Dell Technologies Services, un agent du support technique demande l'accès à l'appareil, y compris le numéro de demande de service, le cas échéant, ainsi que tout autre appareil ou ID utilisateur.
- La demande d'accès distant est mise en file d'attente dans le back-end jusqu'à ce que la passerelle envoie le message de pulsation de l'appareil au back-end pour le récupérer.
- En réponse, le serveur back-end envoie une réponse qui inclut les informations de demande, l'adresse du serveur back-end et un ID de session unique pour se connecter à la passerelle de connexion sécurisée.
- La passerelle de connexion sécurisée utilise son référentiel local pour déterminer l'adresse IP locale de l'appareil. Ensuite, elle vérifie la stratégie mise en cache à partir de Policy Manager pour examiner les autorisations de connexion.
- Si cela est autorisé, la passerelle de connexion sécurisée établit une connexion TLS persistante séparée vers le serveur back-end. La connexion TLS est toujours lancée via la passerelle de connexion sécurisée. Le serveur back-end ne peut jamais lancer une connexion entrante vers le serveur de passerelle. Cela permet de s'assurer qu'il n'y a aucune faille de sécurité face aux attaques externes.

La communication traverse le tunnel entre la passerelle de connexion sécurisée et le serveur back-end jusqu'à ce qu'elle soit terminée ou interrompue après une période d'inactivité.

Sécurité réseau

Tous les composants réseau se trouvent derrière un pare-feu et sont gérés par notre équipe de sécurité réseau. Le trafic réseau est étroitement contrôlé. Tout le trafic entrant est transmis via des ports spécifiques et uniquement envoyé vers les adresses réseau de destination appropriées.

4-3. Stockage, utilisation et processus sécurisés des données

Sécurité pour le stockage et l'utilisation

Sécurité physique

Dell Technologies Services héberge la plupart des données de la passerelle de connexion sécurisée, y compris l'application, les systèmes, le réseau et les composants de sécurité, dans un datacenter basé aux États-Unis, conçu pour maintenir de hauts niveaux de disponibilité et de sécurité. Les données sont protégées à l'aide d'un large éventail de mesures, notamment la sécurité physique. Les fonctionnalités sont notamment les suivantes :

- Gardes de sécurité sur site
- Appareil photo et webcam
- Fausses entrées
- Blocages de véhicules
- Conception d'un parking spécialisé
- Verre et murs à l'épreuve des balles
- Utilisation d'un bâtiment non marqué

L'accès aux datacenters où se trouve l'infrastructure est limité au personnel autorisé et est contrôlé via une carte à puce.

Sécurité logique

Les données générées par la passerelle de connexion sécurisée sont stockées dans le respect de la politique de confidentialité Dell.

L'accès logique à l'infrastructure de Dell Technologies Services (serveurs, équilibreurs de charge, partages réseau, etc.) est limité par le biais d'outils internes audités et évalués conformément aux directives informatiques.

Sécurité logique - Suite

- **Sécurité des serveurs et des bases de données :** les serveurs et les composants du système d'exploitation résident sur des images standard qui ont fait l'objet de tests de sécurité. Les mises à jour de sécurité utilisées par l'application sont régulièrement revues, y compris celles publiées par Microsoft et d'autres éditeurs de logiciels. Lorsque des mises à jour de sécurité critiques sont émises, elles sont d'abord testées sur des images hors production et généralement appliquées aux serveurs en temps réel afin d'éviter les risques.
- **Audit :** les journaux d'appareils de surveillance propriétaires sont conservés et accessibles uniquement par l'infrastructure et les applications Dell Technologies Services. Ces journaux consignent toutes les tentatives de connexion ou d'accès au système d'exploitation ou à la console de serveur Web de la passerelle de connexion sécurisée.

Les builds gérés par le département IT sont renforcées à l'aide des pratiques d'excellence recommandées du Center for Internet Security (CIS). Des consignes de sécurité conformes aux normes du secteur sont également mises en œuvre sur tous les serveurs et tous les équipements réseau.

Enfin, l'écosystème de la passerelle de connexion sécurisée utilise à la fois à la haute disponibilité locale au sein de son datacenter et à une infrastructure identique dans un datacenter distinct. Les seules exceptions sont les technologies offrant une haute disponibilité intrinsèque, telles que les clusters de Big Data et les Clouds privés. Pour l'analytique des données, Dell Technologies Services exploite les environnements Cloud que nous contrôlons et gérons entièrement, y compris les Clouds privés, hybrides et publics.

Authentification

Pour la passerelle de connexion sécurisée, l'authentification auprès de Dell Technologies Services utilise Dell MyAccount et les groupes de connexion du système d'exploitation pour l'authentification « on-the-box ».

Les groupes, tels que l'équipe d'administration des bases de données et l'équipe de support opérationnel, qui ont accès aux composants de la passerelle de connexion sécurisée, sont affectés à des tâches et à des droits d'accès distincts. Toutes les mises à jour de l'environnement de production passent par une procédure de contrôle des changements définie qui intègre des vérifications et des équilibres.

Nous utilisons un processus de développement sécurisé et reproductible pour les produits et les applications

Sécurité pour les processus

Communauté sensibilisée à la sécurité

Nous proposons un programme de formation sur la sécurité multiniveau basé sur des rôles pour former les nouveaux collaborateurs et les collaborateurs existants aux pratiques d'excellence en matière de sécurité et à l'utilisation des ressources appropriées. Dell Technologies s'attache à instaurer une culture de la sécurité au sein de la communauté. En outre, notre communauté de développeurs fait partie du programme Security Champion de Dell qui est conçu pour favoriser la sécurité d'anticipation dans nos pratiques de développement logiciel.

Développement

Notre **norme de Cycle de vie de développement sécurisé (SDL, Secure Development Lifecycle)** est un point de référence commun pour les organisations de produits Dell Technologies afin de comparer les activités de développement sécurisées des produits et des applications aux attentes du marché et aux pratiques du secteur. Elle définit les contrôles de sécurité que les équipes de produits doivent adopter tout en développant de nouvelles fonctions et fonctionnalités. La norme SDL inclut à la fois les activités d'analyse et les contrôles proactifs normatifs concernant les principaux domaines à risque. Les activités d'analyse, telles que la modélisation des menaces, l'analyse de code statique, la numérisation et les tests de sécurité, sont conçues pour détecter et résoudre les problèmes de sécurité tout au long du cycle de vie du développement. Les contrôles normatifs sont destinés à garantir que les équipes de développement codent de manière défensive afin d'éviter les problèmes de sécurité spécifiques, notamment ceux qui se trouvent dans le OWASP (Open Web Application Security Project) Top 10 ou SANS Top 25. La passerelle de connexion sécurisée a adopté

Développement - Suite

le cadre de maturité Dell SDL pour sa mise en œuvre des contrôles de sécurité, conformément aux normes du secteur.

Le code de la passerelle de connexion sécurisée est mis au point à l'aide de la méthodologie de développement agile. Le code est intégré en continu à l'aide d'un logiciel d'automatisation conforme aux normes du secteur. Les versions de code sont archivées et contrôlées à l'aide d'autorisations de groupe sécurisées.

Chaque version logicielle subit une évaluation de la sécurité conformément à nos stratégies de sécurité et inclut :

- L'évaluation des failles de sécurité à l'aide du test d'intrusion
- Des tests de sécurité tiers qui utilisent plusieurs fournisseurs haut de gamme, tels que SecureWorks
- L'évaluation des solutions d'authentification, d'autorisation et de gestion des identités
- Toutes les bibliothèques et tous les composants tiers sont analysés avec des solutions leaders sur le marché pour l'analyse de la composition des logiciels. En outre, les avis de sécurité Dell sont communiqués pour des améliorations de sécurité spécifiques.
- La classification des données avec notre organisation de sécurité mondiale. Ce processus permet de rassembler la confidentialité et la sécurité afin de garantir la protection des données électroniques

Les applications sont également soumises à des audits de sécurité et à la gouvernance.

Gestion des changements

Le processus de gestion des changements Dell Technologies suit les bonnes pratiques de la Fondation ITIL, telles que dictées par son conseil de gestion des changements d'entreprise. Tous les changements sont gérés via des tickets de demande. Les personnes qui accèdent à notre système pour effectuer des changements doivent suivre une formation ITIL, et se familiariser avec SDL. Les versions de toutes les mises à jour et mises à niveau appliquées à l'infrastructure dorsale sont contrôlées pour assurer un suivi et une traçabilité appropriés. L'équipe utilise un processus de création automatisé pour appliquer de nouvelles versions ou révoquer toute version ou tout correctif qui a été déployé.

L'application installée sur le site d'un client peut être mise à niveau en fonction des préférences du client. Chaque version promue à l'adresse Dell.com/support contient des informations sur les changements apportés avec toutes les limitations connues.

Tous les nouveaux changements et fonctionnalités sont traités par notre équipe de gestion des produits et sont hiérarchisés à l'aide d'un processus de changement de plan d'enregistrement qui passe par le comité de contrôle des modifications pour examen et approbation.

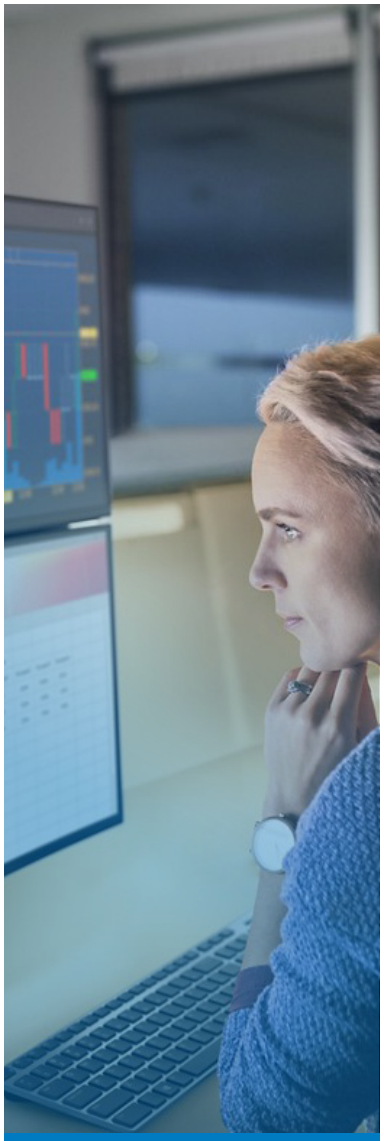
Gestion des risques de la chaîne d'approvisionnement

Dell Technologies suit les bonnes pratiques leaders sur le marché à chaque niveau du cycle de vie planifier-approvisionner-fabriquer-livrer-retourner. Nous adoptons une approche globale et complète de la sécurisation de notre chaîne d'approvisionnement, notamment la mise en place de normes SCRM internationales et de bonnes pratiques, afin de demeurer un fournisseur de technologies de pointe fiable sur le marché mondial.

Pour en savoir plus sur nos pratiques d'assurance de la chaîne d'approvisionnement, cliquez ici.

Rapports sur les incidents

Toute personne chez Dell Technologies qui observe des activités suspectes ou soupçonne un problème de cybersécurité ou une menace est tenue de signaler immédiatement l'incident à notre équipe de réponse aux incidents de sécurité informatique (CSIRT). Cela inclut une faiblesse ou une lacune dans un processus de sécurité qui peut avoir un impact sur notre environnement ou, entraînant une faille des systèmes et/ou des données. Le CSIRT lance alors une consultation complète dans l'incident, et la personne qui signale l'incident fournit tous les artéfacts et les détails nécessaires à l'équipe CSIRT pour mener la procédure d'enquête. L'équipe CSIRT utilise le programme de réponse aux incidents de l'équipe CSIRT qui détaille un processus formel pour contrer et résoudre les incidents de cybersécurité internes et non orientés client. Ces incidents peuvent engendrer des menaces potentielles pour les actifs, les réseaux informatiques ou les équipements de traitement des données Dell, ainsi que pour les informations de Dell et de ses filiales applicables, di personnel, du prestataire de services, du partenaire ou du client.



Collaboration du secteur sur les bonnes pratiques en matière de sécurité des produits

Réponse aux failles de sécurité

Dell Technologies s'efforce d'aider ses clients à minimiser les risques associés aux failles de sécurité de ses produits en fournissant aux clients des informations, des conseils et des mesures d'atténuation en temps opportun pour résoudre les menaces liées aux failles de sécurité. Notre équipe de réponse aux incidents de sécurité des produits (PSIRT) est responsable de la coordination de la réponse et de la divulgation de toutes les failles de sécurité de produit qui nous ont été signalées. Les divulgations de toutes les failles de sécurité concernant des produits Dell Technologies sont disponibles en ligne.

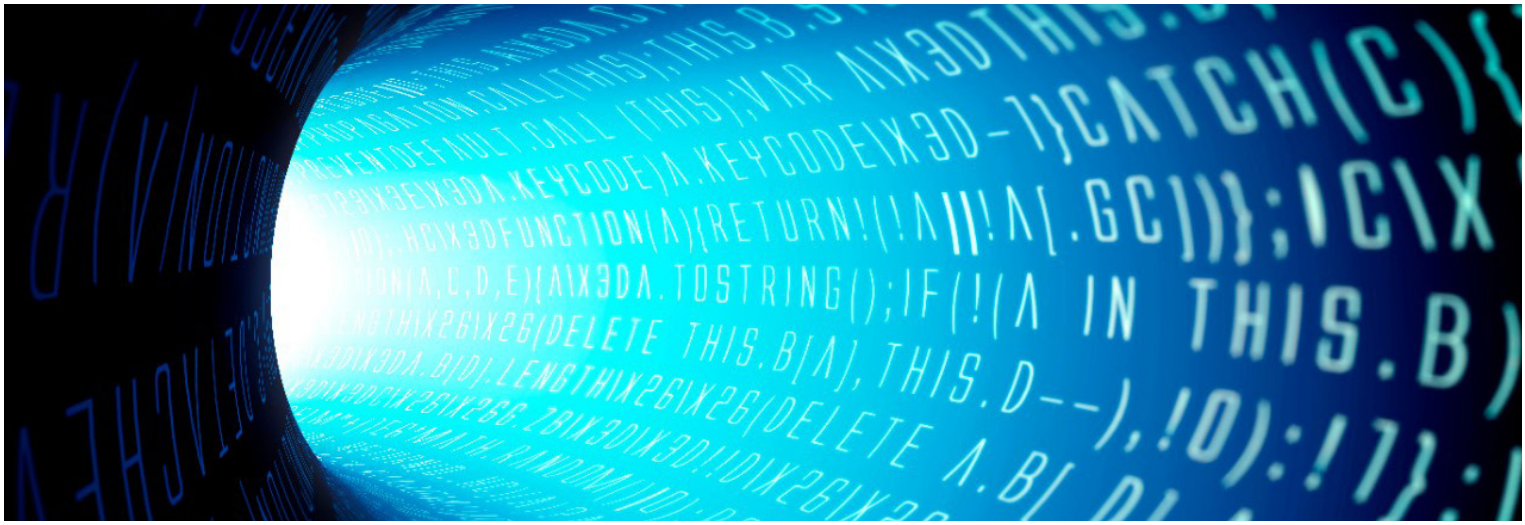
Découvrez plus d'informations sur notre Politique de réponse aux failles de sécurité

Affiliations du secteur

Dell Technologies participe à plusieurs groupes du secteur afin de collaborer avec d'autres fournisseurs leaders dans la définition, l'évolution et le partage des bonnes pratiques en matière de sécurité des produits et d'amélioration de la cause du développement sécurisé. Parmi les exemples de collaboration dans le secteur, citons :

- Dell, par l'intermédiaire de son entité EMC, a co-fondé et préside actuellement le conseil d'administration du Software Assurance Forum for Excellence in code (SAFECode). Les autres membres du conseil d'administration sont des représentants de Microsoft, d'Adobe, de SAP, d'Intel, de Siemens, de CA et de Symantec. Les membres du SAFECode partagent et publient des formations et des pratiques en matière d'assurance logicielle.
- Dell Technologies est un membre actif du Forum for Incident Response and Security Teams (FIRST). FIRST est une organisation de premier plan et un leader mondial reconnu en matière de réponse aux incidents et aux failles de sécurité.
- Nous participons activement à l'Open Group Trusted Technology Forum (OTTF). L'OTTF dirige le développement d'un programme et d'un cadre sur l'intégrité de la chaîne d'approvisionnement mondiale.
- Dell a été l'une des neuf premières entreprises évaluées par le projet BSIMM (Building Security In Maturity Model) en 2008 et a continué de participer au projet. Un représentant de Dell Technologies fait partie du Conseil d'administration du BSIMM.
- Les employés de Dell ont été les membres fondateurs de l'IEEE Center for Secure Design, qui a été lancé dans le cadre de l'initiative de cybersécurité de l'IEEE afin d'aider les architectes logiciels à comprendre et à résoudre les failles de conception de sécurité les plus répandues.

Rendez-vous sur notre Centre de confiance et de sécurité pour consulter des ressources et des solutions pour vous aider à trouver des réponses aux questions de sécurité de votre entreprise.



Normes de sécurité du secteur

Nos employés sont activement impliqués dans les organismes de normalisation et les consortiums du secteur, qui se concentrent sur le développement de normes de sécurité et sur la définition de pratiques de sécurité à l'échelle du secteur, notamment :

- Cloud Security Alliance (CSA)
- Distributed Management Task Force (DMTF)
- Forum for Incident Response and Security Teams (FIRST)
- International Committee for Information Technology Standards (INCITS)
- Organisation internationale de normalisation (ISO)
- Internet Engineering Task Force (IETF)
- The Open Group
- Organization for the Advancement of Structured Information Standards (OASIS)
- Software Assurance Forum for Excellence in Code (SAFECode)
- Storage Networking Industry Association (SNIA)

Certification ISO 9001

Dell Technologies possède la certification ISO 9001. La société réalise régulièrement des audits trimestriels et des examens de conformité pour l'ensemble de ses centres de développement et de fabrication.

5. Conclusion

Notre technologie de connectivité offre une expérience de support informatique sans effort avec des alertes proactives et prédictives automatisées qui garantissent un temps d'activité maximal pour l'infrastructure de datacenter stratégique. Les clients qui collaborent avec Dell Technologies Services bénéficient de notre engagement à offrir une expérience sécurisée et confidentielle pour la collecte, la communication, le transport, l'utilisation et le stockage de leurs données de télémétrie.

Si vous avez des questions ou pour obtenir plus d'informations, visitez le site **DellTechnologies.com/SecureConnectGateway**

1 Source : « The Role Of IT Services Providers Expands To Strategic Collaboration », une étude réalisée par Forrester Consulting pour le compte de Dell Technologies en avril 2021

2 Source : « World Economic Forum Global Risks Report 2021 ». http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf